GREENBERG'S CONJECTURE AND UNITS IN MULTIPLE $\mathbb{Z}_p$-EXTENSIONS

William G. McCallum

June, 2000

Abstract. Let A be the inverse limit of the p-part of the ideal class groups in a $\mathbb{Z}_p^r$-extension K_∞/K. Greenberg conjectures that if r is maximal, then A is pseudo-null as a module over the Iwasawa algebra Λ (that is, has codimension at least 2). We prove this conjecture in the case that K is the field of p-th roots of unity, p has index of irregularity 1, satisfies Vandiver's conjecture, and satisfies a mild additional hypothesis on units. We also show that if K is the field of p-th roots of unity and r is maximal, Greenberg's conjecture for K implies that the maximal p-ramified pro-p-extension of K cannot have a free pro-p quotient of rank r unless p is regular (see also [LN]). Finally, we prove a generalization of a theorem of Iwasawa in the case $r = 1$ concerning the Kummer extension of K_∞ generated by p-power roots of p-units. We show that the Galois group of this extension is torsion-free as a Λ-module if there is only one prime of K above p and K_∞ contains all the p-power roots of unity.

Let K be a number field, let p be an odd prime number, and let $A(K)$ be the p-Sylow subgroup of the ideal class group of K. In 1956, Iwasawa introduced the idea of studying the behaviour of $A(F)$ as F varies over all intermediate fields in a $\mathbb{Z}_p$-extension K_∞/K. Greenberg [G2] gives a comprehensive account of the subsequent development of Iwasawa theory; we recall here some of the basic ideas. The inverse limit $A = \varprojlim_F A(F)$ is a finitely generated torsion module over the Iwasawa algebra $\Lambda = \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]] = \varprojlim_F \mathbb{Z}_p[\mathrm{Gal}(F/K)]$. This algebra has a particularly simple structure: given a topological generator γ of Γ, there is an isomorphism $\Lambda \simeq \mathbb{Z}_p[[T]]$ taking $1+\gamma$ to T. Iwasawa showed that there is a *pseudo-isomorphism* (a map with finite kernel and cokernel) from A to an elementary module $E = \sum_i \Lambda/(f_i)$; the power series $f = \prod_i f_i$ is the *characteristic power series* of A. In [G1], Greenberg conjectured that $f = 1$ when K is totally real.

It is natural to consider the generalization of these ideas to a compositum of $\mathbb{Z}_p$-extensions of K, that is, an extension K_∞/K whose galois group $\Gamma = \mathrm{Gal}(K_\infty/K)$ is isomorphic to $\mathbb{Z}_p^r$ for some positive integer r. The corresponding Iwasawa algebra, $\Lambda = \varprojlim_F \mathbb{Z}_p[\mathrm{Gal}(F/K)]$, is isomorphic to a power series ring in r variables over $\mathbb{Z}_p$. If K is totally real and satisfies Leopoldt's conjecture, then the only $\mathbb{Z}_p$-extension is the cyclotomic one and Greenberg's conjecture that $f = 1$ in this case is equivalent to the statement that A is finite, and hence has annihilator of height 2. More generally, Greenberg has made the following conjecture [G2].

This research was supported in part by an AMS Bicentennial Fellowship and a National Science Foundation grant DMS-9624219.

Conjecture (Greenberg). *Let K_∞/K be the compositum of all $\mathbb{Z}_p$-extensions of K. Then the annilator of A has height at least two.*

A module whose annihilator has height at least 2 is said to be *pseudo-null*. Let $E = \mathcal{O}_K^\times$ and $U = \prod_{\mathfrak{p}|p} \mathcal{O}_{K_\mathfrak{p}}^\times$, and denote by $\overline{E}$ the closure of E in U. The following theorem is a consequence of the main theorem of this paper, Theorem 26.

Theorem **1**. *Let $K = \mathbb{Q}(e^{2\pi i/p})$. Suppose that*

(1) $A(K) \simeq \mathbb{Z}/p\mathbb{Z}$
(2) $(U/\overline{E})[p^\infty] \simeq \mathbb{Z}/p\mathbb{Z}$.

Then K satisfies Greenberg's conjecture.

We note that Greenberg's conjecture is trivially true for regular primes, since in that case $A = 0$. Condition (1) of the theorem implies that p satisfies Vandiver's conjecture, by the reflection principle. The conditions of the theorem are satisfied often (heuristically, by about 3/4 of irregular primes), for example by 37, 59, 67, 101, 103, 131, and 149. More specifically, the conditions are equivalent to the following:

(1) p satisfies Vandiver's conjecture, and divides exactly one of the Bernoulli numbers $B_2, B_4, \ldots, B_{p-1}$
(2) if we write the characteristic series of A for the cyclotomic $\mathbb{Z}_p$-extension in the form $f = (T - cp)u$, where u is a unit power series and γ is chosen to satisfy $\zeta^\gamma = \zeta^{1+p}$ for all p-power roots of unity ζ, then $c \not\equiv 1 \pmod{p}$.

(See [W] Theorem 10.16 and Theorem 8.25.) The computations in [BCEMS] verify Vandiver's conjecture for all primes less than 12,000,000, and condition (1) is satisfied by about 30% of those primes (about 61% of them are regular, in which case $A = 0$). Iwasawa and Sims [IS] tabulate the congruence classes mod p of the p-adic integer c for $1 < p < 400$ and $3600 < p \le 4001$. Condition (2) is satisfied for all primes in their tables that satisfy condition (1).

Greenberg's conjecture may be regarded as a statement about the structure of Galois groups. We call an extension of number fields *p-ramified* if it is unramified outside all the primes above p, and *p-split* if all the primes above p split completely. Let

$$\begin{aligned} M_\infty &= \text{maximal abelian } p\text{-ramified pro-}p\text{-extension of } K_\infty \\ L_\infty &= \text{maximal abelian unramified pro-}p\text{-extension of } K_\infty \\ L'_\infty &= \text{maximal } p\text{-split subextension of } L_\infty/K_\infty \end{aligned}$$

Then the three galois groups

$$Y = \mathrm{Gal}(M_\infty/K_\infty), \quad X = \mathrm{Gal}(L_\infty/K_\infty) \quad \text{and} \quad X' = \mathrm{Gal}(L'_\infty/K_\infty) \tag{1}$$

may be regarded as Λ-modules via the conjugation action of Γ. From class field theory we have a canonical isomorphism of Λ-modules $A \simeq X$. Thus Greenberg's conjecture asserts that X is pseudo-null. This turns to be equivalent to the statement that Y is Λ-torsion-free (see Theorem 3 and Corollary 14), and it is this latter formulation that we prove. The equivalence was communicated to the author by Greenberg, and has been proved independently by Lannuzel and Nguyen Quang Do in [LN].

Greenberg's conjecture has a connection with the structure of $\mathcal{G} = \mathrm{Gal}(\Omega/K)$, where Ω is the maximal p-ramified pro-p extension of K. This connection has been studied by Lannuzel and Nguyen Quang Do in [LN]. It is well-known that $\mathcal{G}$ is the quotient of a free pro-p-group on g generators by s relations, where

$$g = \dim_{\mathbb{Z}/p\mathbb{Z}} H^1(\mathcal{G}, \mathbb{Z}/p\mathbb{Z})$$
$$s = \dim_{\mathbb{Z}/p\mathbb{Z}} H^2(\mathcal{G}, \mathbb{Z}/p\mathbb{Z}),$$

and that g and s are minimal in this regard. Thus $\mathcal{G}$ cannot have a free pro-p quotient of rank greater than $g - s$. On the other hand, $\mathcal{G}$ is free of rank $g - s$ if $s = 0$, that is, in the case $K = \mathbb{Q}(\zeta_p)$, if p is regular.

THEOREM **2**. *Suppose that $\mathbb{Q}(\zeta_p)$ satisfies Greenberg's conjecture. Then $\mathcal{G}$ has a pro-p-free quotient of rank $g - s$ if and only if p is regular.*

This is proved in Section 3. Lannuzel and Nguyen Quang Do prove a similar result for a general ground field K, but under the more restrictive hypothesis that all finite abelian p-ramified extensions of K satisfy Leopoldt's conjecture ([LN], Theorem 5.4.)

In proving that Y is torsion-free, we will make use of the following generalization of a theorem of Iwasawa on units [Iw]. Let

$$N_\infty = K_\infty(\epsilon^{1/p^n} : n \in \mathbb{N}, \epsilon \in \mathcal{O}_{K_\infty}[1/p]^\times).$$

THEOREM **3**. *Suppose that K_∞/K is a multiple $\mathbb{Z}_p$-extension satisfying:*

1. *K_∞ contains all the p^n-th roots of unity, $n > 0$*
2. *there is only one prime of K above p.*

Then the Λ-module $Y' = \mathrm{Gal}(N_\infty/K_\infty)$ is torsion-free. In particular, Y_{tor} fixes N_∞.

Acknowledgements The essential ideas of this work were developed in 1995–96, at the Institute for Advanced Study. The author would like to thank them for their hospitality, Ralph Greenberg and David Marshall for useful comments and conversations, and the referee for suggesting numerous improvements.

1. Ext Groups and Local Cohomology.

In this section we collect together various results from the literature (see, for example, [B-H] and [H]). Let $N = r+1$, the dimension of Λ. Let $\mathfrak{m}$ be the maximal ideal of Λ. Let $\mathbf{x} = x_1, \ldots, x_N$ be a finite sequence in Λ that generates an $\mathfrak{m}$-primary ideal. The Koszul complex

$$0 \xrightarrow{d} K_N(\mathbf{x}) \xrightarrow{d} K_{N-1}(\mathbf{x}) \xrightarrow{d} \cdots \xrightarrow{d} K_1(\mathbf{x}) \xrightarrow{d} K_0(\mathbf{x}) \to 0$$

is defined as follows. Let Λ^N be the free Λ-module with basis $\{e_i : 1 \leq i \leq N\}$. Then

$$K_i(\mathbf{x}) = \bigwedge^i \Lambda^N$$

and

$$d(e_{j_1} \wedge \cdots \wedge e_{j_i}) = \sum_{s=1}^{i} (-1)^{s-1} x_{j_s} e_{j_1} \wedge \cdots \wedge \hat{e}_{j_s} \wedge \cdots \wedge e_{j_i},$$

where the hat indicates that a term is omitted. If $\mathbf{x}$ is a regular sequence, then the Koszul complex is a free resolution of $\Lambda/(\mathbf{x})$ ([Ma], Theorem 43).

Given a finitely generated Λ-module X, we define a complex $K^*(\mathbf{x}, X)$ by

$$K^*(\mathbf{x}, X) = \mathrm{Hom}_\Lambda(K_*(\mathbf{x}), X)$$

and define $H^*(\mathbf{x}, X)$ to be the cohomology of this complex.

Now let $(\mathbf{x}_n)$ be a sequence of sequences

$$\mathbf{x}_n = (x_{n,1}, \ldots, x_{n,N}),$$

such that $x_{n,i} \mid x_{m,i}$, $n \leq m$, $1 \leq i \leq N$. If $n \leq m$, there is a natural map of complexes

$$K_.(\mathbf{x}_n) \to K_.(\mathbf{x}_m),$$

which multiplies $e_{j_1} \wedge \cdots \wedge e_{j_i}$ by

$$\left(\frac{x_{m,j_1}}{x_{n,j_1}}\right) \cdots \left(\frac{x_{m,j_i}}{x_{n,j_i}}\right).$$

Denote by $I(\mathbf{x})$ the ideal of Λ generated by the components of $\mathbf{x}$. Suppose that for each $k \in \mathbb{N}$ there are $i, j \in \mathbb{N}$ such that $I(\mathbf{x}_i) \subset \mathfrak{m}^k$ and $\mathfrak{m}^j \subset I(\mathbf{x}_k)$. Then, for a finitely generated Λ-module X,

$$\varinjlim_n H^i(\mathbf{x}_n, X)$$

is the local cohomology group $H^i_{\mathfrak{m}}(X)$ defined by Grothendieck. This is shown in Sect. 3.5 of [B-H] for the case where $\mathbf{x} = x_1, \ldots, x_N$ is a sequence in Λ that generates an $\mathfrak{m}$-primary ideal and $x_{n,i} = x_i^n$. The construction there generalizes easily to our situation.

Theorem 4 (Grothendieck Duality for Λ). *Suppose that for each positive integer n we have a sequence $\mathbf{x}_n = (x_{n,1}, \ldots, x_{n,N})$ generating an $\mathfrak{m}$-primary ideal, such that $x_{n,i} \mid x_{m,i}$, $n \leq m$, $1 \leq i \leq N$, and such that for each $k \in \mathbb{N}$ there are $i, j \in \mathbb{N}$ such that $I(\mathbf{x}_i) \subset \mathfrak{m}^k$ and $\mathfrak{m}^j \subset I(\mathbf{x}_k)$. Then there is an isomorphism of functors of finitely generated Λ-modules*

$$\mathrm{Ext}_\Lambda^{N-i}(\cdot, \Lambda) \simeq \mathrm{Hom}_{\mathbb{Z}_p}(\varinjlim_n H^i(\mathbf{x}_n, \cdot), \mathbb{Q}/\mathbb{Z}).$$

Proof: This is the version of Grothendieck's local duality theorem suggested by Exercise 3.5.14 of [B-H]. The local duality theorem is [B-H], Theorem 3.5.8. We note that Λ is a regular local ring, so it is *a fortiori* a Cohen-Macaulay local ring, and therefore satisfies the hypotheses of the results in [B-H] cited here. ■

Now let $I \subset \Lambda$ be the augmentation ideal, let $g_1, \ldots, g_r$ be a set of topological generators for Γ, and let $(T_1, \ldots, T_r)$ be the corresponding set of generators for I ($g_i = 1 + T_i$). Let

$$\omega_n(T_i) = (1+T_i)^{p^n} - 1, \quad \nu_n(T_i) = \frac{\omega_n(T_i)}{T_i} \qquad n \geq 0.$$

There are two particularly useful choices of sequence in applying Theorem 4:

$$\mathbf{x}_n = (p^n, \omega_n(T_1), \ldots, \omega_n(T_r)) \quad \text{and} \quad \mathbf{x}_n = (p^n, \nu_n(T_1), \ldots, \nu_n(T_r)).$$

Let

$$\mathbf{x}'_n = (\omega_n(T_1), \ldots, \omega_n(T_r)) \quad (\text{respectively } (\nu_n(T_1), \ldots, \nu_n(T_r))).$$

One easily deduces from the definitions an exact sequence

$$0 \to H^{i-1}(\mathbf{x}'_n, X)/p^n \to H^i(\mathbf{x}_n, X) \to H^i(\mathbf{x}'_n, X)[p^n] \to 0. \tag{2}$$

In the case $i = r$, the map on the right is induced by $(y_0, \ldots, y_r) \mapsto y_0$. Note that, in the case $\mathbf{x}_n = (p^n, \omega_n(T_1), \ldots, \omega_n(T_r))$, $H^r(\mathbf{x}'_n, X) = X/(\omega_n(T_1), \ldots, \omega_n(T_r))$. Define a functor

$$E(X) = \mathrm{Hom}_{\mathbb{Z}_p}(\varinjlim H^r(\mathbf{x}'_n, X), \mathbb{Q}_p/\mathbb{Z}_p).$$

In the case where $r = 1$ and X_n is torsion, $E(X)$ is Iwasawa's original definition of the adjoint module of X. The following proposition is proved in [Mc] (Proposition 2).

Proposition 5. *There is a functorial injective map $E(X) \to \mathrm{Ext}_\Lambda^1(X, \Lambda)$. This map is an isomorphism if $H^r(\mathbf{x}'_n, X)$ is finite for all sufficiently large n.*

We conclude with two lemmas on pseudo-null modules which will be needed later.

Lemma **6**. *Let X be a finitely generated Λ-module. Then X is pseudo-null if and only if X is torsion and* $\operatorname{Ext}^1_\Lambda(X,\Lambda)=0$.

Proof: This is also proved in [H], Theorem 11. Since Λ has dimension $r+1$, it follows from Theorem 4 that X is torsion and $\operatorname{Ext}^1_\Lambda(X,\Lambda)=0$ if and only if $H^{r+1}_{\mathfrak{m}}(X)=H^r_{\mathfrak{m}}(X)=0$, where $\mathfrak{m}\subset\Lambda$ is the maximal ideal and $H^*_{\mathfrak{m}}(\cdot)$ is the local cohomology. By [B-H] Theorem 3.5.7, these two local cohomology groups vanish if and only if the dimension of X as a Λ-module is less than or equal to $r-1$. Since R is a regular local ring, the dimension of X is $r+1$ minus the height of its annihilator ([B-H], Corollary 2.1.4), hence the dimension of X is less than or equal to $r-1$ if and only if the height of the annihilator of X is at least 2, that is, if and only if X is pseudo-null. ■

Lemma **7**. *Let X be a finitely-generated torsion Λ-module. Then X is pseudo-isomorphic to* $\operatorname{Ext}^1(X)$. *Further,* $\operatorname{Ext}^1(X)$ *is pseudo-null if and only if it is zero.*

Proof: There is a pseudo-isomorphism $X\to E$, where E is an elementary module, that is, a product of modules of the form $\Lambda/(f)$, $f\in\Lambda$. Taking $\operatorname{Ext}^*(\cdot)$ of the sequence

$$0\to\Lambda\xrightarrow{f}\Lambda\to\Lambda/(f)\to 0,$$

we see that $\operatorname{Ext}^1(\Lambda/(f))=\Lambda/(f)$ if $f\neq 0$. Hence, for any elementary torsion-module E, $\operatorname{Ext}^1(E)\simeq E$. Now, a pseudo-isomorphism

$$X\to E$$

leads to a map

$$\operatorname{Ext}^1(E)\to\operatorname{Ext}^1(X),$$

which is a pseudo-isomorphism, since Ext^i of a pseudo-null module is pseudo-null for any i (the annihilator of X also annihilates its Ext groups). Thus $\operatorname{Ext}^1(X,\Lambda)$ is pseudo-isomorphic to X. The second statement of the lemma now follows immediately from Lemma 6. ■

2. The Direct Limit of the Ideal Class Group.

Let X' be as in (1). For a positive integer n, let K_n be the fixed field of $p^n\Gamma$. Let $X'_n=X'_{K_n}$. Define ideals ω_n and $\nu_{n,m}$ in Λ by

$$\omega_n=(\omega_n(T_1),\ldots,\omega_n(T_r))$$
$$\nu_{n,m}=(\nu_{n,m}(T_1),\ldots,\nu_{n,m}(T_r)),\quad \nu_{n,m}(T)=\frac{\omega_n(T)}{\omega_m(T)}.$$

From (2) we get a surjective map

$$H^r(\mathbf{x}_n,X')\twoheadrightarrow X'/\omega_nX'[p^n]$$

and, composing this with the natural map

$$X'/\omega_n X' \to X'_n, \tag{3}$$

we get a map

$$H^r(\mathbf{x}_n, X') \to X'_n[p^n].$$

Theorem **8**. *Suppose that K has only one prime above p. Then the natural map*

$$H^r(\mathbf{x}_n, X') \to X'_n[p^n]$$

induces an isomorphism

$$\varinjlim_n H^r(\mathbf{x}_n, X') \simeq \varinjlim X'_n[p^n] = \varinjlim X'_n.$$

In particular, $\mathrm{Ext}^1(X')$ *is the Pontryagin dual of* $\varinjlim X'_n$.

Proof: Since there is only one prime of K above p, its decomposition group in Γ has finite index. Choose n_0 large enough so that all the primes above p are totally ramified in K_∞/K_{n_0}. Then (3) is surjective, hence the direct limit of $H^r(\mathbf{x}_n, X') \to X'_n[p^n]$ surjective also. Thus it suffices to show that the direct limit is injective.

Choose a fixed prime $\mathfrak{p}$ of L' above p. Since L'/K_∞ is p-split, the decomposition group of $\mathfrak{p}$ in $\mathrm{Gal}(L'/K_n)$ is isomorphic to $\Gamma_{K_n} = p^n\Gamma$; in particular, it is abelian. Denote this decomposition group by $\tilde{\Gamma}_{\mathfrak{p},n}$.

Suppose that $n \geq n_0$. We claim that the kernel of $X'/\omega_n X' \to X'_n$ is contained in $\nu_{n,n_0} X'/\omega_n X'$. First, since $\mathrm{Gal}(L'/K_n) = \tilde{\Gamma}_{\mathfrak{p},n} X'$ and $\tilde{\Gamma}_{\mathfrak{p},n}$ is abelian, the commutator subgroup of $\mathrm{Gal}(L'/K_n)$ is $\omega_n X'$. Thus $X'/\omega_n X'$ is the maximal abelian quotient of $\mathrm{Gal}(L'/K_n)$, and hence the kernel of $X'/\omega_n X' \to X'_n$ is generated by the decomposition groups above p. Since there is only one prime of K above p, all the decomposition groups are conjugate under the action of Γ. Thus, the subgroup of X' generated by the decomposition groups is generated by commutators $[\gamma, g']$, where $\gamma \in \tilde{\Gamma}_{\mathfrak{p},n}$ and $g' \in \mathrm{Gal}(L'/K)$. Furthermore, we can restrict γ to a set of generators of $\tilde{\Gamma}_{\mathfrak{p},n}$. Now, as noted above, the image of $\tilde{\Gamma}_{\mathfrak{p},n}$ in Γ is $p^n\Gamma$. So we may assume that the image of γ in Γ is $g_i^{p^n}$ for some i. Choose g so that

$$g^{p^{n_0}} = \gamma_0 x \qquad \gamma_0^{p^{n-n_0}} = \gamma$$

for some $\gamma_0 \in \tilde{\Gamma}_{\mathfrak{p},n_0}$ and some $x \in X'$. Let T (resp. T') be the image of $1-g$ (resp. $1-g'$) in Λ. Then, using the commutator identity

$$[a^N, b] = [a,b]^{a^{N-1}}[a,b]^{a^{N-2}} \dots [a,b],$$

we find

$$\nu_{n_0}(T)[g,g'] = [g^{p^{n_0}}, g'] = [\gamma_0 x, g'] = [\gamma_0, g'] + [x, g'] = [\gamma_0, g'] + T'x.$$

Thus

$$\nu_n(T)[g,g'] = \nu_{n,n_0}(T)([\gamma_0, g'] + T'x) = \\ [\gamma_0^{p^{n-n_0}}, g'] + \nu_{n,n_0}(T)T'x = [\gamma, g'] + \nu_{n,n_0}(T)T'x.$$

Hence, since $[g,g'] \in X'$ and ν_{n,n_0} divides ν_n, $[\gamma, g'] \in \nu_{n,n_0}(T)X'$. This proves the claim.

We apply the results of Section 1 using

$$\mathbf{x}_n = (p^n, \omega_n(T_1), \ldots, \omega_n(T_r)).$$

and

$$\mathbf{y}_n = (p^n, \nu_{n,n_0}(T_1), \ldots, \nu_{n,n_0}(T_r)).$$

The fact that the kernel of $X'/\omega_n X' \to X'_n$ is contained in $\nu_{n,n_0}X'/\omega_n X'$ implies that $H^r(\mathbf{y}'_n, X)$ is a quotient of X'_n. Hence it is finite, so by Proposition 5,

$$\varinjlim H^r(\mathbf{y}'_n, X') \simeq D = \mathrm{Hom}(\mathrm{Ext}^1(X'), \mathbb{Q}_p/\mathbb{Z}_p).$$

On the other hand, it follows from Theorem 4 that

$$D \simeq \varinjlim_n H^r(\mathbf{x}_n, X').$$

Hence

$$\varinjlim_n H^r(\mathbf{x}_n, X') \simeq \varinjlim_n H^r(\mathbf{y}'_n, X').$$

Since $H^r(\mathbf{x}_n, X') \to H^r(\mathbf{y}'_n, X')$ factors through the $X'_n \to H^r(\mathbf{y}'_n, X')$, this implies that $\varinjlim_n H^r(\mathbf{x}_n, X') \to \varinjlim_n X'_n$ is injective. This concludes the proof of the theorem. ■

3. Interpretation of Greenberg's Conjecture in Terms of Y.

For each prime $\mathfrak{p}$ of K lying above p, let $r_{\mathfrak{p}}$ be the integer such that the decomposition group $\Gamma_{\mathfrak{p}}$ of $\mathfrak{p}$ in Γ is isomorphic to $\mathbb{Z}_p^{r_{\mathfrak{p}}}$. Let Y and X' be as in (1). For any Λ-module M and $i \in \mathbb{Z}$ we denote by $M(i)$ the i-th Tate twist of M.

THEOREM **9**. *Suppose that K_∞ contains the p^n-th roots of unity for every positive integer n, and that $r_{\mathfrak{p}} \geq 2$ for all primes $\mathfrak{p}$ of K lying above p. Then $\mathrm{Ext}^1_\Lambda(X', \Lambda)(1)$ is pseudo-isomorphic to Y_{tor}, and is isomorphic to Y_{tor} if $r_{\mathfrak{p}} \geq 3$ for all $\mathfrak{p}$.*

In order to prove Theorem 9, we relate $\mathrm{Ext}^1(Y,\Lambda)$ to X' using a duality theorem of Jannsen [J2]. Then we use a basic structure theorem for Y to turn this around into a relation between Y_{tor} and $\mathrm{Ext}^1(X',\Lambda)$. The structure theorem, due independently to Jannsen [J1] and Nguyen-Quang-Do [Ng], may be formulated conveniently in terms of an auxiliary Iwasawa-module Z, defined by Nguyen-Quang-Do [Ng].

Theorem **10** ([J1], [Ng]). *Suppose that K_∞ contains the p^n-th roots of unity for every positive integer n. There is a Λ-module Z with a presentation*

$$0 \to \Lambda^s \to \Lambda^g \to Z \to 0, \tag{4}$$

for some non-negative integers s and g, such that Y fits in a short exact sequence

$$0 \to Y \to Z \to I \to 0,$$

where $I \subset \Lambda$ is the augmentation ideal.

We define Z as follows. Let Ω be the maximal p-ramified pro-p-extension of K, $\mathcal{G} = \mathrm{Gal}(\Omega/K)$, and $\mathcal{I}$ the augmentation ideal in $\mathbb{Z}_p[[\mathcal{G}]]$. Define

$$Z_F = H_0(\Omega/F, \mathcal{I}), \qquad Z = Z_{K_\infty}.$$

If $K \subset F \subset K_\infty$, the identification

$$H_0(\mathrm{Gal}(K_\infty/F), Z) = Z_F$$

gives a natural surjective map

$$Z \twoheadrightarrow Z_F.$$

Let Y_F be the Galois group of the maximal abelian p-ramified pro-p extension of F. Denote by I_F the augmentation ideal in $\mathbb{Z}[\mathrm{Gal}(F/K)]$. By taking $\mathrm{Gal}(\Omega/F)$ homology of the exact sequence

$$0 \to \mathcal{I} \to \mathbb{Z}_p[[\mathcal{G}]] \to \mathbb{Z}_p \to 0,$$

one obtains an exact sequence

$$0 \to Y_F \to Z_F \to I_F \to 0, \tag{5}$$

functorial in F.

In particular, with $F = K_\infty$, we obtain the second sequence in the statement of the theorem. The integers g and s in the theorem are

$$g = \dim_{\mathbb{Z}/p\mathbb{Z}} H^1(\mathcal{G}, \mathbb{Z}/p\mathbb{Z})$$
$$s = \dim_{\mathbb{Z}/p\mathbb{Z}} H^2(\mathcal{G}, \mathbb{Z}/p\mathbb{Z})$$

As explained in [Ng], (4) may be derived from the presentation of $\mathcal{G}$ as a pro-p group with g generators and s relations. (Injectivity on the left in (4) depends on the assumption that K_∞ contains all p-power roots of unity, which implies that K_∞ satisfies the weak Leopoldt conjecture, $H^2(K_\infty, \mathbb{Q}_p/\mathbb{Z}_p) = 0$; see [Ng] for details.)

The presentation (4) allows us to compute $\mathrm{Ext}^i(Y) = \mathrm{Ext}^i_\Lambda(Y,\Lambda)$ for $i \geq 2$. Although it is not needed in what follows, the answer is simple so we present it here.

Proposition **11**. *Let* $r = \operatorname{rank}_{\mathbb{Z}_p} \Gamma$. *If* $i \geq 2$, *then*

$$\operatorname{Ext}^i(Y) = \begin{cases} 0 & i \neq r-2 \\ \mathbb{Z}_p & i = r-2. \end{cases}$$

Proof: Since Z has a free resolution of length 2, $\operatorname{Ext}^i(Z) = 0$ if $i \geq 2$. Thus, taking Ext of (5) with $F = K_\infty$, we see that $\operatorname{Ext}^i(Y) \simeq \operatorname{Ext}^{i+1}(I)$ if $i \geq 2$. Now use the following lemma. ■

Lemma **12**. *If* $i \geq 1$, *then*

$$\operatorname{Ext}^i(I) = \begin{cases} 0 & i \neq r-1 \\ \mathbb{Z}_p & i = r-1. \end{cases}$$

Proof: Taking Ext of

$$0 \to I \to \Lambda \to \mathbb{Z}_p \to 0,$$

we see that $\operatorname{Ext}^i(I) \simeq \operatorname{Ext}^{i+1}(\mathbb{Z}_p)$ if $i \geq 1$. But, using the Koszul resolution of $\mathbb{Z}_p$, one can see that this latter group is zero unless $i+1 = r$, in which case it is $\mathbb{Z}_p$. ■

The structure of $\operatorname{Ext}^i(Y)$ when $i = 1$ is more subtle. A duality theorem between X' and Y, due to Jannsen, relates it to the Iwasawa module

$$H^2_\infty = \varprojlim_F H^2(\mathcal{O}'_F, \mathbb{Z}_p(1)),$$

which is related to X' by the exact sequence

$$0 \to X' \to H^2_\infty \to \sum_{\mathfrak{p}|p} \mathbb{Z}_p[[\Gamma/\Gamma_\mathfrak{p}]] \to \mathbb{Z}_p \to 0, \tag{6}$$

where the sum is over all primes of K dividing p. We denote by $X(n)$ the usual Tate twist of a Λ-module X by $\mathbb{Z}_p(1)^{\otimes n}$, where $\mathbb{Z}_p(1) = \varprojlim \mu_{p^n}$.

Theorem **13** ([J2], Theorem 5.4d). *If* $r \neq 2, 3$, *there is an isomorphism*

$$H^2_\infty \simeq \operatorname{Ext}^1(Y, \Lambda)(1).$$

If $r = 2$ *there is an exact sequence*

$$\mathbb{Z}_p(1) \to H^2_\infty \to \operatorname{Ext}^1(Y, \Lambda)(1) \to 0,$$

and if $r = 3$, *there is an exact sequence*

$$0 \to H^2_\infty \to \operatorname{Ext}^1(Y, \Lambda)(1) \to \mathbb{Z}_p(1).$$

Proof of Theorem 9: Let $\mathfrak{p}$ be a prime of K lying above p. The annihilator of $\Lambda_{\mathfrak{p}} = \mathbb{Z}_p[[\Gamma/\Gamma_{\mathfrak{p}}]]$ as a Λ-module is the augmentation ideal in $\mathbb{Z}_p[[\Gamma_{\mathfrak{p}}]]$, which has height $r_{\mathfrak{p}}$. Thus, the hypothesis on $r_{\mathfrak{p}}$ implies that $\Lambda_{\mathfrak{p}}$ is pseudo-null, and hence has vanishing Ext^1 by Lemma 6. Furthermore, if $r_{\mathfrak{p}} \geq 3$ then its Ext^2 vanishes as well—the argument for this is entirely similar to that in the proof of Lemma 6. There is a natural surjection $X \to X'$, whose kernel is generated as a $\mathbb{Z}_p$-module by the Frobenius automorphisms corresponding to primes above p, and is therefore a finitely generated module over $\bigoplus_{\mathfrak{p}} \Lambda_{\mathfrak{p}}$. Hence the kernel is pseudo-null, and so $\mathrm{Ext}^1(X)$ is isomorphic to $\mathrm{Ext}^1(X')$.

From (6) we get an injection $X' \hookrightarrow H^2_\infty$ whose cokernel is pseudo-null, and has vanishing Ext^2 if $r_{\mathfrak{p}} \geq 3$ for all $\mathfrak{p}$. Thus $\mathrm{Ext}^1(X')$ is pseudo-isomorphic to $\mathrm{Ext}^1(H^2_\infty)$, and is isomorphic if $r_{\mathfrak{p}} \geq 3$ for all $\mathfrak{p}$.

Since $\mathbb{Z}_p(1)$ has vanishing Ext^1 when $r \geq 2$ and vanishing Ext^2 when $r \geq 3$, Theorem 13 implies that $\mathrm{Ext}^1(H^2_\infty)(1)$ is isomorphic to $\mathrm{Ext}^1(\mathrm{Ext}^1(Y))$. It follows from (5) and Lemma 12 that there is a pseudo-isomorphism $\mathrm{Ext}^1(Z) \to \mathrm{Ext}^1(Y)$. Furthermore, this is an injection with cokernel $\mathbb{Z}_p$ if $r = 3$, and an isomorphism if $r > 3$. Hence from Lemma 7 that $\mathrm{Ext}^1(\mathrm{Ext}^1(Y))$ is pseudo-isomorphic to $\mathrm{Ext}^1(\mathrm{Ext}^1(Z))$, isomorphic if $r \geq 3$. An elementary calculation with the two-step free resolution of Z shows that

$$\mathrm{Ext}^1(\mathrm{Ext}^1(Z)) \simeq Z_{\mathrm{tor}}.$$

Finally, it follows from (4) that $Z_{\mathrm{tor}} \simeq Y_{\mathrm{tor}}$. ■

Corollary **14**. *Suppose that K_∞ contains the p^n-th roots of unity for every positive integer n, and that $r_{\mathfrak{p}} \geq 2$ for all primes $\mathfrak{p}$ of K lying above p. Then Greenberg's conjecture is satisfied if and only if $Y_{\mathrm{tor}} = 0$.*

Proof: Theorem 9 and Lemma 7 imply the corollary directly in the case $r_{\mathfrak{p}} \geq 3$. In the case $r_{\mathfrak{p}} = 2$ they imply that Greenberg's conjecture is equivalent to the pseudo-nullity of Y_{tor}. However, since K_∞ contains μ_{p^∞}, it verifies the weak Leopoldt conjecture, hence Y has no non-trivial pseudo-null submodule (see [Ng]), so Y_{tor} is pseudo-null if and only if it is zero. ■

This result has also been shown in [LN]. We conclude this section by proving Theorem 2, which we restate here for convenience.

Theorem **2**. *Suppose that $\mathbb{Q}(\zeta_p)$ satisfies Greenberg's conjecture. Then $\mathcal{G}$ has a pro-p-free quotient of rank $g - s$ if and only if p is regular.*

Proof: Suppose that there is a surjective map $\mathcal{G} \to \mathcal{F}$, where $\mathcal{F}$ is a free group of rank $g - s$. Then, from the definition of Z, we see that there is a surjective map $Z \to \Lambda^{g-s}$. On the other hand, Z has rank $g - s$, so we must have

$$Z \simeq \Lambda^{g-s} \oplus Z_{\mathrm{tor}}.$$

By Corollary 14, $Y_{\rm tor} = 0$, so Z is free. Since $Z/IZ \simeq Z_K \simeq Y_K \simeq \mathcal{G}^{\rm ab}$, this implies that the maximal abelian p-ramified p-extension of K has Galois group isomorphic to $\mathbb{Z}_p^{g-s}$; in particular, there is no torsion in the Galois group. It follows from the theory of cyclotomic fields that p is regular (see, for example, the proof of Lemma 25). ■

4. A Generalization of Iwasawa's Theorem on Units.

In this section we prove Theorem 3, whose statement we recall here. Recall

$$N_\infty = K_\infty(\epsilon^{1/p^n} : n \in \mathbb{N}, \epsilon \in \mathcal{O}_{K_\infty}[1/p]^\times).$$

THEOREM **3**. *Suppose that K_∞/K is a multiple $\mathbb{Z}_p$-extension satisfying:*

(1) *K_∞ contains all the p^n-th roots of unity, $n > 0$*
(2) *there is only one prime of K above p.*

Then the Λ-module $Y' = \mathrm{Gal}(N_\infty/K_\infty)$ is torsion-free. In particular, $Y_{\rm tor}$ fixes N_∞.

For a finite extension F/K contained in K_∞, let $E_F = \mathcal{O}_F[1/p]^\times$, and let $E_F^u \subset E_F$ be the group of universal norms, that is, the elements of E_F that are norms of elements of E_L for every extension L/F contained in K_∞/F. Let $\mathcal{E} = \varinjlim_F E_F$, and consider the subgroup $\mathcal{E}^u = \varinjlim_F E_F^u \subset \mathcal{E}$. Define N_∞^u to be the extension of K_∞ obtained by adjoining all p-power roots of all elements of $\mathcal{E}^u$, and let $Y^u = \mathrm{Gal}(N_\infty^u/K_\infty)$.

LEMMA **15**. *Suppose that K_∞ contains all p-power roots of unity. Then Y^u is Λ-torsion free.*

Proof: From Kummer theory, we have an isomorphism of Λ-modules

$$Y^u \simeq \mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{E}^u \otimes \mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p(1)).$$

Let $E = \varprojlim_F E_F^u = \varprojlim_F E_F$, regarded as a Λ-module. We define a homomorphism

$$\mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{E}^u \otimes \mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p(1)) \to \mathrm{Hom}_\Lambda(E, \Lambda(1)) \tag{7}$$

by mapping χ to the homomorphism

$$(u_F) \mapsto (\sum_{\sigma \in \mathrm{Gal}(F/K)} q(F)_* \chi(u_F^\sigma \otimes q(F)^{-1})\sigma),$$

where $q(F)$ is the number p-power roots of unity in F, and

$$q(F)_* : q(F)^{-1}\mathbb{Z}/\mathbb{Z} \to \mathbb{Z}/q(F)\mathbb{Z}$$

is induced by multiplication by $q(F)$. Since every universal norm $u \in E_F^u$ occurs as part of a norm compatible sequence, χ is in the kernel of this map if and only if $\chi = 0$, hence (7) is injective. The lemma now follows from the fact that $\mathrm{Hom}_\Lambda(E, \Lambda(1))$ is torsion-free, since $\Lambda(1)$ is free of rank 1. ■

It follows from the lemma that the torsion submodule of Y' is contained in the kernel of $Y' \to Y^u$, which, by Kummer theory, is the Pontriagin dual of $\varinjlim_F (E_F/E_F^u) \otimes \mathbb{Q}_p/\mathbb{Z}_p$. We prove Theorem 3 by showing that the direct limit is zero. We define a filtration $E_F^u \subset E_F^n \subset E_F^{\mathrm{loc}} \subset E_F$ by

$$\begin{aligned} E_F^n &= \{x \in E_F : x \in N_{L/F} L^\times \text{ for all finite } L/F \text{ in } K_\infty\} \\ E_F^{\mathrm{loc}} &= \{x \in E_F : x_v \in N_{L_v/F_v} L_v^\times, \text{ all finite } L/F \text{ in } K_\infty, \text{ all valuations } v \text{ of } L\} \end{aligned}$$

We show $\varinjlim_F (E_F/E_F^u) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$ by considering each graded piece in turn. We make use of the following lemmas, whose proofs are elementary and left to the reader:

LEMMA **16**. *Suppose that (M_j), $j \in J$, is a direct system of $\mathbb{Z}_p$-modules, and that for every positive integer n and every j there exists $j' \geq j$ such that the image of*

$$M_j \to M_{j'}$$

is contained in $p^n M_{j'}$. Then

$$\varinjlim_j M_j \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0.$$

For abelian groups $H \subset \Gamma$ of finite index, define

$$e(\Gamma, H) = \frac{\text{index of } H \text{ in } \Gamma}{(\text{exponent of } \Gamma/H)}.$$

LEMMA **17**. *If $\Gamma \simeq \mathbb{Z}_p^r$ with $r > 1$, then*

$$\lim_H e(\Gamma, H) = p^\infty,$$

where the limit is over open neighborhoods H of the identity.

Units modulo local norms. Let $\Gamma_F = \mathrm{Gal}(K_\infty/F)$, and, for a prime $\mathfrak{p}$ of F, denote by $\Gamma_{F,p}$ the decomposition group of $\mathfrak{p}$ in Γ_F (where the context removes ambiguity, we denote $\Gamma_{F,\mathfrak{p}}$ simply by $\Gamma_\mathfrak{p}$).

Proposition **18**. *Suppose that $r \geq 2$ and that there is only one prime of K lying above p. Then*

$$\varinjlim((E_F/E_F^{\mathrm{loc}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p) = 0.$$

Proof: Recall that Y_F and X'_F are the Galois groups respectively of the maximal abelian p-ramified pro-p-extension of F, and the maximal abelian unramified pro-p-extension in which all primes above p split completely. By class field theory we have an exact sequence

$$E_F \otimes \mathbb{Z}_p \to \prod_{\mathfrak{p}|p} \mathrm{Gal}(\overline{F}_{\mathfrak{p}}^{\mathrm{ab}}/F_{\mathfrak{p}}) \to Y_F \to X'_F \to 0,$$

where the map on the left is the product of the local reciprocity maps over all primes of F above p. Let $H_{\mathfrak{p}}$ be the kernel of $\mathrm{Gal}(\overline{F}_{\mathfrak{p}}^{\mathrm{ab}}/F_{\mathfrak{p}}) \to \Gamma_{F,\mathfrak{p}}$. The reciprocity map takes an element to $H_{\mathfrak{p}}$ if and only if it is a local universal norm at $\mathfrak{p}$. Let $H_F \subset Y_F$ be the image of $\prod_{\mathfrak{p}} H_{\mathfrak{p}}$ and let $W_F = Y_F/H_F$. Then we get an exact sequence

$$0 \to E_F/E_F^{\mathrm{loc}} \otimes \mathbb{Z}_p \to \prod_{\mathfrak{p}} \Gamma_{F,\mathfrak{p}} \to W_F \to X'_F \to 0.$$

Thus it suffices to show that

$$\varinjlim_F \prod_{\mathfrak{p}} \Gamma_{F,\mathfrak{p}} \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$$

and

$$\varinjlim_F W_{F,\mathrm{tor}} \hookrightarrow \varinjlim_F X'_F.$$

The first follows easily from Lemmas 17 and 16, since, for an extension F'/F contained in K_∞, the transition map $\Gamma_{F,\mathfrak{p}} \to \Gamma_{F',p}$ is the transfer, which is multiplication by the index $[\Gamma_{F,\mathfrak{p}} : \Gamma_{F',p}]$. Hence its image lies in $e(\Gamma_{F,\mathfrak{p}}, \Gamma_{F',p})\Gamma_{F',p}$.

To prove the second, note that $\varprojlim \Gamma_{F,\mathfrak{p}} = 0$, hence

$$\varprojlim_F W_F = X' = \mathrm{Gal}(L'/K_\infty),$$

where L' and X' are as in (1). Let K_n be as in Section 2, and let $\tilde{\Gamma}_{\mathfrak{p},n}$ be a decomposition group of $\mathfrak{p}$ in $\mathrm{Gal}(L'/K_n)$. Choose n large enough so that all the primes above p are totally ramified in K_∞/K_n. Then, as pointed out in the proof of Theorem 8, the commutator subgroup of $\mathrm{Gal}(L'/K_n)$ is $\omega_n X'$. Hence we have an exact sequence

$$0 \to X'/\omega_n X' \to W_{K_n} \to \Gamma_{K_n}.$$

Since Γ_{K_n} is torsion-free, $W_{K_n,\mathrm{tor}} \subset X'/\omega_n X'$.

Thus it suffices to show that

$$\varinjlim_n (X'/\omega_n X')_{\text{tor}} \hookrightarrow \varinjlim_n X'_n,$$

or, equivalently, that

$$\varinjlim_n (X'/\omega_n X')[p^n] \hookrightarrow \varinjlim_n X'_n[p^n].$$

Since the map

$$(X'/\omega_n X')[p^n] \to X'_n[p^n]$$

is a factor of

$$H^r(\mathbf{x}_n, X') \twoheadrightarrow (X'/\omega_n X')[p^n] \to X'_n[p^n],$$

this follows from Theorem 8.

■

Local norms modulo global norms.

For a $\mathbb{Z}_p$-module M, let $M^\wedge$ denote $\mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$.

Lemma **19**. *Suppose that no prime splits completely in K_∞/K. Let F/K be a finite subextension of K_∞/K. There is a surjective map of* $\mathrm{Gal}(F/K)$*-modules*

$$H^2(\Gamma_F, \mathbb{Q}_p/\mathbb{Z}_p)^\wedge \twoheadrightarrow \frac{E_F^{\mathrm{loc}}}{E_F^n}.$$

Proof: Let $\mathbf{I}_F$ be the idèle group of F and let $\mathbf{C}_F = \mathbf{I}_F/F^\times$ be the idèle class group. It follows from the hypothesis, and the fact that K_∞/K is unramified outside p, that any element of $F^\times$ that is a universal local norm must be a p-unit, and so E_F^{loc}/E_F^n is the kernel of

$$\varprojlim_L \hat{H}^0(L/F, L^\times) \to \varprojlim_L \hat{H}^0(L/F, \mathbf{I}_L),$$

where the limit is taken over all finite extension L/F in K_∞. Taking $\mathrm{Gal}(L/F)$-cohomology of the exact sequence

$$0 \to L^\times \to \mathbf{I}_L \to \mathbf{C}_L \to 0$$

yields an exact sequence

$$\hat{H}^{-1}(L/F, \mathbf{C}_L) \to \hat{H}^0(L/F, L^\times) \to \hat{H}^0(L/F, \mathbf{I}_L).$$

By class field theory,

$$\hat{H}^{-1}(L/F, \mathbf{C}_L) = \hat{H}^{-3}(L/F, \mathbb{Z}) = H^2(L/F, \mathbb{Q}/\mathbb{Z})^\wedge = H^2(L/F, \mathbb{Q}_p/\mathbb{Z}_p)^\wedge.$$

Thus E_F^{loc}/E_F^n is a quotient of

$$\varprojlim_L H^2(L/F, \mathbb{Q}_p/\mathbb{Z}_p)^\wedge = (\varinjlim H^2(L/F, \mathbb{Q}_p/\mathbb{Z}_p))^\wedge = H^2(\Gamma_F, \mathbb{Q}_p/\mathbb{Z}_p)^\wedge.$$

■

Lemma **20**. *Let Γ be an abelian group isomorphic to $\mathbb{Z}_p^r$ and let Γ' be a subgroup of Γ of finite index. Then the image of $H^2(\Gamma, \mathbb{Q}_p/\mathbb{Z}_p)^\wedge \to H^2(\Gamma', \mathbb{Q}_p/\mathbb{Z}_p)^\wedge$ (dual to the corestriction map) is contained in $e(\Gamma, \Gamma')H^2(\Gamma', \mathbb{Q}_p, \mathbb{Z}_p)^\wedge$.*

Proof: Dually, we prove that the corestriction map

$$H^2(\Gamma', \mathbb{Q}_p/\mathbb{Z}_p) \to H^2(\Gamma, \mathbb{Q}_p/\mathbb{Z}_p)$$

vanishes on $H^2(\Gamma', \mathbb{Q}_p/\mathbb{Z}_p)[e(\Gamma, \Gamma')]$. It is shown in [Br] that $H^2(\Gamma', \mathbb{Q}_p/\mathbb{Z}_p)$ is generated by cup products of characters $\chi_1', \chi_2' \in H^1(\Gamma', \mathbb{Q}_p/\mathbb{Z}_p)$. Furthermore, if $e(\Gamma, \Gamma')$ kills $\chi_1' \cup \chi_2'$, then it kills one of the characters, say χ_2'. The corestriction map on characters is composition with the transfer map $\Gamma \to \Gamma'$, which is just multiplication by $[\Gamma : \Gamma']$ in this case. If we write $\chi_i' = \operatorname{res} \chi_i$ for some characters χ_i of Γ, $i = 1, 2$, and let $p^e = \operatorname{ord}(\chi_2)/\operatorname{ord}(\chi_2')$, then p^e divides the exponent of Γ/Γ', and

$$\operatorname{cores}(\chi_1' \cup \chi_2') = (\chi_1 \cup \operatorname{cores} \chi_2') = [\Gamma : \Gamma'](\chi_1 \cup \chi_2).$$

Now, since $e_2(\Gamma, \Gamma')$ kills χ_2', $p^e e_2(\Gamma, \Gamma')$ kills χ_2. But p^e divides the exponent of Γ/Γ', and hence $p^e e_2(\Gamma, \Gamma')$ divides $[\Gamma : \Gamma']$, hence $[\Gamma : \Gamma']$ kills χ_2. Thus the right hand side of the displayed equation is zero, as required. ∎

Proposition **21**. *Suppose that K_∞ contains all p-power roots of unity and that $r \geq 2$. Then the direct system $(E_F^{\text{loc}}/E_F^n) \otimes \mathbb{Z}_p$ satisfies the conditions of Lemma 16, and hence $\varinjlim (E_F^{\text{loc}}/E_F^n) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$.*

Proof: This follows from Lemma 19 and Lemma 20. ∎

Global norms modulo norms of units.

Lemma **22**. *Let F/K be a finite extension contained in K_∞. There is a surjective map of $\operatorname{Gal}(F/K)$-modules*

$$H_1(\Gamma_F, X') \twoheadrightarrow \frac{E_F^n}{E_F^u}.$$

Proof: Let I_F be the group of ideals in $\mathcal{O}_F[1/p]$, P_F the group of principal ideals, and $C_F' = I_F/P_F$. For a finite extension L/F in K_∞, consider the exact sequences

$$0 \to E_L \to L^\times \to P_L \to 0$$

and

$$0 \to P_L \to I_L \to C_L' \to 0.$$

Since I_L is a direct sum of induced $\operatorname{Gal}(L/F)$-modules, it is cohomologically trivial. Hence cohomology of the second sequence yields

$$H_1(L/F, C_L') = \hat{H}^{-2}(L/F, C_L') \simeq \hat{H}^{-1}(L/F, P_L).$$

Cohomology of the first sequence gives

$$\hat{H}^{-1}(L/F, P_L) \to \hat{H}^0(L/F, E_L) \to \hat{H}^0(L/F, L^\times).$$

Splicing these together we get

$$H_1(L/F, C'_L) \to \frac{E_F \cap N_{L/F} L^\times}{N_{L/F} E_L} \to 0.$$

Taking the inverse limit over L, and noting that, since L/F is a p-extension, $H_1(L/F, C'_L) \simeq H_1(L/F, A'_L)$, we obtain the required map. ■

Remark. If K_n is as in Section 2, then

$$H_1(\Gamma_{K_n}, X') = H^{r-1}(\mathbf{x}'_n, X'),$$

where $\mathbf{x}'_n = (\omega_n(T_1), \ldots, \omega_n(T_r))$.

PROPOSITION **23**. *Suppose K has exactly one prime above p. Then $\varinjlim (E_F^n/E_F^u) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$.*

Proof: From Lemma 22 and the remark above it suffices to prove that

$$\varinjlim_n H^{r-1}(\mathbf{x}'_n, X') \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0.$$

The exact sequence (2) with $i = r$ yields

$$0 \to H^{r-1}(\mathbf{x}'_n, X')/p^n \to H^r(\mathbf{x}_n, X') \to (X'/\omega_n X')[p^n] \to 0.$$

Theorem 8 implies the direct limit of the right hand arrow is an isomorphism; hence the direct limit of the group on the left is zero. ■

Proof of Theorem 3: The case $r = 1$ follows from [Iw, Theorem 15]. Hence we may assume $r \geq 2$. Recall from the discussion at the beginnning of this section that Y^u is torsion-free, and that the kernel of $Y' \to Y^u$ is the Pontriagin dual of $\varinjlim_F (E_F/E_F^u) \otimes \mathbb{Q}_p/\mathbb{Z}_p$. It follows from Propositions 18, 21, and 23 that this direct limit is zero, and hence the theorem follows.

5. A Criterion for the Vanishing of Y_{tor}.

We recall the notation of Section 3, in particular

$$g = \dim_{\mathbb{Z}/p\mathbb{Z}} H^1(\mathcal{G}, \mathbb{Z}/p\mathbb{Z})$$
$$s = \dim_{\mathbb{Z}/p\mathbb{Z}} H^2(\mathcal{G}, \mathbb{Z}/p\mathbb{Z})$$

Note that if $s = 0$, then, by (4), Z is a free Λ-module, hence $Y_{\mathrm{tor}} = 0$. Our aim is to develop a test in the next simplest case. Let K^{ab} be the maximal abelian p-ramified pro-p-extension of K.

LEMMA **24**. *Suppose that K satisfies Leopoldt's conjecture and that $s = 1$. If Y_{tor} fixes K^{ab}, then $Y_{\text{tor}} = 0$.*

Proof: Since $s = 1$, the resolution of Z looks like

$$0 \to \Lambda \to \Lambda^g \to Z \to 0. \tag{8}$$

Let $\lambda = (\lambda_1, \dots, \lambda_g)$ be the image of 1 under the left hand map in this resolution. Choose an element $y \in Y_{\text{tor}}$ such that if $y = fy'$, $f \in \Lambda$, $f, y' \neq 0$, then f is a unit in Λ. Let $(\mu_1, \dots, \mu_g) \in \Lambda^g$ map to y. Then the μ_i are relatively prime, and there exist $f, h \in \Lambda$, $f \neq 0$, such that

$$f \cdot (\mu_1, \dots, \mu_g) = h \cdot (\lambda_1, \dots, \lambda_g).$$

Since Λ is a unique factorization domain and the μ_i are relatively prime, h divides f; replacing f by f/h we get

$$f \cdot (\mu_1, \dots, \mu_g) = (\lambda_1, \dots, \lambda_g). \tag{9}$$

(This last step depended on the assumption $s = 1$ in a crucial way.) Now take $H_0(\Gamma, \cdot)$ of the sequence (8), noting that from (5) we have $H_0(\Gamma, Z) = Z_K = Y_K = \text{Gal}(K^{\text{ab}}/K)$:

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{i} \mathbb{Z}_p^g \longrightarrow \text{Gal}(K^{\text{ab}}/K) \longrightarrow 0$$

The fact that i is injective is a consequence of Leopoldt's conjecture. Indeed, as explained in [Ng], the kernel, $H_1(K_\infty/K, Z)$, is isomorphic to the Pontriagin dual of $H^2(K, \mathbb{Q}_p/\mathbb{Z}_p)$, and the vanishing of this latter cohomology group is an equivalent formulation of Leopoldt's conjecture. We have $i(1) = \lambda(0)$; since i is injective, $\lambda(0) \neq 0$. It follows that $f(0) \neq 0$. Since $f(0)\mu(0) = \lambda(0)$, the power of p dividing $f(0)$ is the order of the image of $\mu(0)$ in $\text{Gal}(K^{\text{ab}}/K)$. By hypothesis, that order is 1, hence $f(0)$ is a unit. Hence f itself is a unit power series, and thus $y = 0$. ∎

In view of Theorem 3, our first step in applying the criterion developed in Lemma 24 is to restrict ourselves to a class of multiple $\mathbb{Z}_p$-extensions K_∞/K for which $K^{\text{ab}} \subset N_\infty$. The following lemma gives one such class of extensions. Recall that A is the p-primary part of the ideal class group of K, $E = \mathcal{O}_K^\times$, $U = \prod_{\mathfrak{p}|p} \mathcal{O}_{K_\mathfrak{p}}^\times$, and that $\overline{E}$ is the closure of E in U.

LEMMA **25**. *Suppose that $K = \mathbb{Q}(\zeta_p)$.*

1. *Suppose that $A(K) \simeq \mathbb{Z}/p\mathbb{Z}$. Then $s = 1$.*
2. *Suppose further that $(U/\overline{E})[p^\infty] \simeq \mathbb{Z}/p\mathbb{Z}$. Then $G^{\text{ab}}[p^\infty] \simeq \mathbb{Z}/p\mathbb{Z}$.*
3. *Suppose further that K_∞ contains the p^n-th roots of unity for all $n > 0$. Then $K^{\text{ab}} \subset N_\infty$.*

Proof: (1) We must show that $H^2(\mathcal{G}, \mathbb{Z}/p\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}$. Since $\mu_p \subset K$, we have $H^2(\mathcal{G}, \mathbb{Z}/p\mathbb{Z}) \simeq H^2(\mathcal{G}, \mu_p)$. The latter may be calculated by regarding it as an étale cohomology group over $S = \mathrm{Spec}(\mathcal{O}[1/p])$, and using the Kummer sequence of étale sheaves on S

$$1 \to \mu_p \to \mathbb{G}_\mathrm{m} \to \mathbb{G}_\mathrm{m} \to 1.$$

Let C be the ideal class group of K. Since the prime of K above p is principal, we have $C \simeq \mathrm{Pic}(\mathcal{O}_K[1/p]) \simeq H^1_{\text{ét}}(S, \mathbb{G}_\mathrm{m})$. Furthermore, $H^2_{\text{ét}}(S, \mathbb{G}_\mathrm{m}) = 0$, since it is the Brauer group of S, and may be identified with the subgroup of the Brauer group of K unramified outside p. Since there is only one prime above p and K is totally complex, this subgroup is zero. Thus $H^1_{\text{ét}}(S, \mu_p) \simeq C/pC \simeq A/pA$.

(2) From class field theory we have an exact sequence

$$0 \to U^{(1)}/\overline{E^{(1)}} \to G^{\mathrm{ab}} \to A \to 0,$$

where U is the group of units in the completion of K at the prime above p, and $\overline{E}$ is the closure of the global units in U, and the superscript 1 indicates that we take units congruent to 1 modulo p. Let $(\alpha) = \mathfrak{a}^p$ where $\mathfrak{a}$ is an ideal of K representing a generator a for $A(K)$. Write $\alpha = \alpha' u$ for some $u \in \mu_{p-1}(K_\mathfrak{p})$, $\alpha' \in U^{(1)}$. If a lifts to $\overline{a} \in G^{\mathrm{ab}}$, then $\overline{a}^p \in U^{(1)}/\overline{E^{(1)}}$ is represented by α'. Since $\alpha \neq 1$ and $\mu_{p-1}(K) = \{1\}$, $\alpha' \neq 1$. It follows that the image of $\alpha_\mathfrak{p}$ in $U^{(1)}/\overline{E^{(1)}}$ is not a torsion element. Indeed, $\mathfrak{a} \in A(i)$ where i is odd and $i \neq 1$, hence $\overline{E^{(1)}}(i) = 0$. Therefore, all the torsion in G^{ab} is contained in $U^{(1)}/\overline{E^{(1)}}$.

(3) Let $\tilde{K}$ denote the compositum of all $\mathbb{Z}_p$-extensions of K. We will first show that $\tilde{K}$ is contained in the field obtained by adjoining p-power roots of p-units to $K(\mu_{p^\infty}) \subset K_\infty$. Indeed, let

$$\omega : \mathbb{Z}_p^\times \to \mu_{p-1}(\mathbb{Z}_p)$$

be the Teichmuller character (characterized by $\omega(a) \equiv a \pmod{p}$). Let (ζ_n) be a generator of $\mathbb{Z}_p(1) = \varprojlim \mu_{p^n}$, and let

$$\eta_{k,n} = \prod_{a \in (\mathbb{Z}/p^n\mathbb{Z})^\times} (1 - \zeta_n^a)^{\omega^k(a)a^{-1}}.$$

(Here a^{-1} denotes any integer congruent to a^{-1} modulo p^n.) Then $\eta_{k,n}$ is a p-unit in $\mathbb{Q}(\mu_{p^n})$. Further $G_n = \mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/K)$ acts on the class of $\eta_{k,n}$ in $\mathbb{Q}(\mu_{p^n})^\times/\mathbb{Q}(\mu_{p^n})^{\times p^n}$ via the cyclotomic character, and $\Delta = \mathrm{Gal}(K/\mathbb{Q})$ acts via the character ω^{-k}. Hence, by Kummer theory, the p^n-th root of $\eta_{k,n}$ generates an extension $L_n/\mathbb{Q}(\mu_{p^n})$ on which G_n acts trivially, and which is therefore abelian over K. Thus $L_n = K(\mu_{p^n})K_n$ for some p-extension K_n/K such that Δ acts on $\mathrm{Gal}(K_n/K)$ via ω^{k+1}. Furthermore, if $m > n$,

$$N_{\mathbb{Q}(\mu_{p^m})/\mathbb{Q}(\mu_{p^n})} \eta_{k,m} = \eta_{k,n}^{p^{m-n}},$$

so $K_n \subset K_m$, and the union of K_n, $n > 1$, forms an extension of K which is either trivial or is a $\mathbb{Z}_p$-extension on which Δ acts by ω^{k+1}. In fact the extension is non-trivial precisely when $k = p-2$ (the cyclotomic $\mathbb{Z}_p$-extension) or when $0 \le k \le p-1$ and k is even. The compositum of all these extensions has galois group $\mathbb{Z}_p^{(p+1)/2}$, the maximal allowable rank by class field theory. Hence it is $\tilde{K}$, and is visibly contained in N_∞.

By definition, $\mathrm{Gal}(\tilde{K}/K)$ is the torsion-free quotient of G^{ab}, so it follows from (2) that $\mathrm{Gal}(K^{\mathrm{ab}}/\tilde{K}) \simeq \mathbb{Z}/p\mathbb{Z}$. On the other hand, we can generate a p-ramified extension of $\tilde{K}$ whose galois group is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ simply by taking the extension $K(\alpha^{1/p})$, where α is as in (2). This extension is a non-trivial p-ramified extension (it is not contained in $\tilde{K}$ because of eigenspace considerations) and is abelian over K since $\alpha \in K$. Thus $K^{\mathrm{ab}} = \tilde{K}(\alpha^{1/p})$. We claim that $\mathfrak{a}$ capitulates in K_∞. This implies that α can be written as a p-th power times a unit in K_∞, and thus $\alpha^{1/p} \in N_\infty$. Since we have already seen that $\tilde{K} \subset N_\infty$, this proves the lemma.

To prove the claim, we show that K_∞ contains H, the p-Hilbert class field of K. It follows from well-known results in the theory of cyclotomic fields that H is generated by the p^{th}-th root of a cyclotomic unit. (The reflection principle, [W], Theorem 10.9, implies that p does not divide h^+. The claim now follows from Theorems 10.16, 8.2, and 8.25.) Since the p-th roots of all the cyclotomic units in K are contained in K_∞, this implies that $H \subset K_\infty$. ∎

6. The Main Theorem.

THEOREM **26**. *Let K_∞/K be a multiple $\mathbb{Z}_p$-extension of K, $\mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p^r$, $r \ge 2$. Suppose that K and K_∞ satisfy the following conditions:*

(1) *K_∞ contains all p-power roots of unity*
(2) *there is only one prime of K above p*
(3) *K satisfies Leopoldt's conjecture*
(4) $\dim_{\mathbb{Z}/p\mathbb{Z}} H^2(\mathcal{G}, \mathbb{Z}/p\mathbb{Z}) = 1$
(5) *the maximal abelian p-ramified pro-p extension of K is contained in*

$$N_\infty = (K_\infty(\epsilon^{1/p^n} : n \in \mathbb{N}, \epsilon \in \mathcal{O}_{K_\infty}[1/p]^\times)$$

Then A is a pseudo-null Λ-module.

Proof: It follows from Theorem 3 that Y_{tor} fixes N_∞. Since $K^{\mathrm{ab}} \subset N_\infty$, it follows from Lemma 24 that $Y_{\mathrm{tor}} = 0$. The theorem follows from Corollary 14 (note that since K has only one prime above p, $r_{\mathfrak{p}} = r \ge 2$). ∎

Proof of Theorem 1: Let $K = \mathbb{Q}(\zeta_p)$ and suppose that K satisfies conditions (1) and (2) in the statement of Theorem 1. Let K_∞ be the compositum of all $\mathbb{Z}_p$-extensions of K. Trivially, conditions (1) and (2) of Theorem 26 are satisfied. Condition (3), Leopoldt's conjecture, is well-known ([W], Theorem 5.25). Finally, by Lemma 25, conditions (4) and (5) of Theorem 26 are satisfied.

Bibliography

[**Br**] K. S. Brown, *Cohomology of Groups*, Springer-Verlag, New York, 1982.

[**B-H**] W. Bruns & J. Herzog, *Cohen-Macaulay rings, Cambridge studies in advanced mathematics* **39**, Cambridge University Press, Cambridge, 1993.

[**BCEMS**] J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä, M. A. Shokrollahi, *Irregular Primes and Cyclotomic Invariants to 12 Million*, J. Symbolic Computation **31** (2001), 89–96.

[**G1**] R. Greenberg, *On the Iwasawa Invariants of Totally Real Number Fields*, Amer. J. Math. **98, No. 1** (1976), 263–284.

[**G2**] ———, *Iwasawa Theory—Past and Present*, `\vrule width0pt\href{http://www.math.washington.edu}{http://www.mat` `/~greenber`.

[**H**] J. A. Hillman, *Alexander Ideals of Links, Lecture Notes in Mathematics* **895**, Springer-Verlag, Berlin, 1981.

[**Iw**] K. Iwasawa, *On $\mathbb{Z}_\ell$-extensions of algebraic number fields*, Annals of Math. **98** (1973), 246–326.

[**IS**] K. Iwasawa and C. C. Sims, *Computation of invariants in the theory of cyclotomic fields*, J. Math. Soc. Japan **18, No. 1** (1966), 86–96.

[**J1**] U. Jannsen, *On the structure of Galois groups as Galois modules*, in Number Theory Noordwijkerhout 1983, Lecture Notes in Math. **1068**, Springer, Berlin, 1984, pp. 109–126.

[**J2**] ———, *Iwasawa Modules up to Isomorphism*, in Advanced Studies in Pure Mathematics **17**, Academic Press, Orlando, 1989, pp. 171-207.

[**LN**] A. Lannuzel & T. Nguyen Quang Do, *Conjectures de Greenberg et extensions pro-p-libres d'un corps de nombres*, to appear in Manuscripta Mathematica.

[**Mc**] W. G. McCallum, *Duality Theorems in the Multivariable Iwasawa Theory of Number Fields,* `\vrule width0pt\href{http://www.math.arizona.edu\string~wmc}{http://www.math.arizona.edu$\sim$wmc}`.

[**Ma**] H. Matsumura, *Commutative Algebra*, Benjamin, Reading, 1980.

[**Ng**] T. Nguyen-Quang-Do, *Formations de classes et modules d'Iwasawa*, Number Theory Noordwijkerhout, 1983, Lecture Notes in Math. **1068**, Springer, Berlin, 1984, pp. 167-185.

[**W**] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York, 1982.

Department of Mathematics, University of Arizona, Tucson, AZ, 85721